# TTP Detail – T1071

## TTP Information

Name: Application Layer Protocol

Description: Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, DNS, or publishing/subscribing. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.(Citation: Mandiant APT29 Eye Spy Email Nov 22)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control

## Malware

* Clambling
* Duqu
* Hildegard
* Lucifer
* NETEAGLE
* Nightdoor
* QUIETEXIT
* Raspberry Robin
* Siloscape

## Tools

* Sliver

## APTs (Intrusion Sets)

* INC Ransom
* Magic Hound
* Rocke
* TeamTNT
* Velvet Ant